CLAIMS

1. An arrangement for protection of end user personal profile data in a communication system comprising a number of end user stations and a number of service/information/content providers or holding means holding end user personal profile data,
c h a r a c t e r i z e d i n
that it comprises an intermediate proxy server supporting a first communication protocol for end user station communication and comprising means for providing published certificates,
a personal profile data protection server supporting a second communication protocol for communication with the intermediary proxy server and a third communication protocol for communication with a service/information/content provider, and an application programming interface (API) allowing service/information/content provider queries/interactions, and comprising storing means for storing of end user specific data and end user personal profile data, and in that the intermediary proxy server comprises means for verifying the genuinity of a certificate requested over said second communication protocol from the personal profile protection server against a published certificate and in that the service/information content server can request, via the API, personal profile data and in that personal profile data is delivered according to end user preferences or in such a manner that there is no association between the actual end user and the personal profile data of the end user.

2. An arrangement according to claim 1,
c h a r a c t e r i z e d i n
that the first communications protocol is a secure protocol.

3. An arrangement according to claim 1 or 2,

c h a r a c t e r i z e d i n
that the first protocol is HTTP or WSP/HTTPS.

4. An arrangement according to any one of claims 1-3,
c h a r a c t e r i z e d i n
that the second communication protocol is a non-secure protocol, e.g. HTTP etc.

5. An arrangement according to any one of clams 1-3,
c h a r a c t e r i z e d i n
that the second protocol is a secure protocol, e.g. HTTP-S or IP Sec.

6. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the end user station is a mobile telephone, e.g. a WAP-telephone, or a fixed station, e.g. a PC, or any other mobile or fixed device.

7. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the intermediary proxy server is a HTTP proxy.

8. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the intermediary proxy server comprises holding means for holding published certificates.

9. An arrangement according to any one of claims 1-7,
c h a r a c t e r i z e d i n
that the intermediary proxy server is in communication with external holding means holding published certificates.

10. An arrangement according to any one of the preceding claims, c h a r a c t e r i z e d i n that the intermediary proxy server is located at, or associated with, the end user station.

11. An arrangement according to any one of claims 1-9, c h a r a c t e r i z e d i n that the intermediary proxy server is located within an intranet or at the operator's premises.

12. An arrangement according to any one of the preceding claims, c h a r a c t e r i z e d i n that the intermediary proxy server comprises a functionality for establishing a security communication agreement (e.g. P3P or a natural language agreement) with the protection server.

13. An arrangement according to claim 12, c h a r a c t e r i z e d i n that the user preferences are stored in the end user station.

14. An arrangement according to claim 12, c h a r a c t e r i z e d i n that the user preferences relating to privacy level are stored in the intermediary proxy server.

15. An arrangement according to claim 13 or 14, c h a r a c t e r i z e d i n that the user preferences relating to privacy level are stored in separate fast access storing means after completion of the security communication agreement.

16. An arrangement according to any one of the preceding claims, c h a r a c t e r i z e d i n

that the protection server comprises an API allowing service provider control of site and page policies, and in that if the end user privacy level is increased, data below the privacy level is deleted.

17. An arrangement according to claim 16,
c h a r a c t e r i z e d i n
that the protection proxy server provides certificates, and preferably signatures upon request by said intermediary proxy server.

18. An arrangement according to claim 17,
c h a r a c t e r i z e d i n
that the protection proxy server comprises, or is associated with holding means for holding security agreements, e.g. P3P statements.

19. An arrangement according to any one of claims 16-18,
c h a r a c t e r i z e d i n
that it comprises an API, e.g. SQL, allowing service provider queries to the storing means (according to policy settings of the service provider).

20. An arrangement according to claim 19,
c h a r a c t e r i z e d i n
that the protection server storing means comprises at least three tables containing information about end user specific data, personal profile data information and statistical data respectively.

21. An arrangement according to claim 19 or 20,
c h a r a c t e r i z e d i n

that end user specific data and end user personal profile data is provided to the service provider in such a manner that the end user cannot be traced, i.e. without end user association.

22. An arrangement according to claim 21,
c h a r a c t e r i z e d i n
that the protection proxy server comprises means for pseudonymizing statistical information and personal profile information by using a unique pseudo for each URL of the service provider that is requested.

23. A method for protection of end user personal profile data in a communication system with a number of end user stations and a number of service/information/content providers,
c h a r a c t e r i z e d i n
that it comprises the steps of:

- registering a certificate for an end user personal profile protection server with a trusted third party,
- providing a request for the certificate (and signed content) from an intermediary proxy server in communication with an end user station using a first communication protocol, to the protection server over a second communication protocol,
- providing a response from the protection server to the intermediary server,
- verifying, in the intermediary proxy server that the certificate is genuine, i.e. belongs to the respective protection server and is registered with the trusted third party,
- after confirmation that the protection server/ certificate is genuine,
- allowing the service provider having acquired the protection server to retrieve end user data and personal profile data according to policy setting and end user privacy level over

an Application Programming Interface and a third communication protocol.

24. The method according to claim 23,
c h a r a c t e r i z e d i n
that it further comprises the step of:
- establishing an end user personal profile data security agreement between the intermediary proxy server and the protection server (on behalf of the end user and the service provider).

25. The method according to claim 24,
c h a r a c t e r i z e d i n
that the agreement comprises a P3P agreement.

26. The method according to claim 24,
c h a r a c t e r i z e d i n
that the agreement comprises a natural language agreement.

27. The method according to any one of claims 23-26,
c h a r a c t e r i z e d i n
that the first and second communication protocols are secure, e.g. HTTP-S and/or IP Sec.

28. The method according to any one of claims 23-27,
c h a r a c t e r i z e d i n
that the first and/or communication protocol is HTTP, WSP or similar, secure version or not.

29. The method according to any one of claims 23-28,
c h a r a c t e r i z e d i n

that the end user preferences (privacy levels) are stored in the end user station or in the intermediary proxy server, and in that they can be separately stored after confirmation of the agreement.

30. The method according to any one of claims 23-29,
c h a r a c t e r i z e d i n
that it comprises the steps of:
- providing an API at the protection server,
- using the API for queries to the protection servers from the service provider,
- providing responses over a third communication protocol to the service provider.

31. The method of claim 30,
c h a r a c t e r i z e d i n
that it comprises the steps of:
- storing data in a number of tables in the protection server relating to user specific data, end user personal profile data and statistical data.

32. The method of claim 31,
c h a r a c t e r i z e d i n
that it comprises the step of:
- pseudonymizing statistical data and profile information such that end user personal data cannot be associated or tied to the actual end user.